OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER

for

British Columbia

2001 / 2002 ANNUAL REPORT

DOC
BC
I4606
B
2001/02
c.3

LEGISLATIVE LIBRARY MAY 3 1 2002

Canadian cataloguing in Publication Data British Columbia.
Office of the Information and Privacy Commissioner.
Annual Report – 1993/1994 –

Annual Report year ends March 31.
First Report covers eight month period from Aug. 1, 1993 - March 31, 1994

ISSN 1198-5909 - Annual Report British Columbia.
Office of the Information & Privacy Commissioner.

1. British Columbia. Office of the Information & Privacy Commissioner – Periodicals.
2. Privacy, Right of – British Columbia – Periodicals.
3. Government information – British Columbia – Periodicals.
4. Public records – British Columbia – Periodicals.
5. British Columbia. Freedom of Information and Protection of Privacy Act. I. Title

KEB505.52 342.711'062 C94-960212-4
KF5753.I5B74

LEGISLATIVE LIBRARY OF BRITISH COLUMBIA
3 3298 00264 8880
102-05478/

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

May 30, 2002

The Honourable Claude Richmond
Speaker
Legislative Assembly of British Columbia
Victoria, BC V8V 1X4

Dear Honourable Speaker Richmond:

Pursuant to section 51 of the *Freedom of Information and Protection of Privacy Act*, I have the honour to present the Office's ninth Annual Report to the Legislative Assembly. This report covers the period from April 1, 2001 to March 31, 2002.

Yours sincerely,

David Loukidelis
Information and Privacy Commissioner
for British Columbia

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Fourth Floor, 1675 Douglas Street
Telephone: (250) 387-5629 Facsimile: (250) 3874696
Toll Free enquiries through *Enquiry BC* at (800) 6637867 or (604) 660-2421 (Vancouver)
website: http//www.oipcbc.org

Table of Contents

SECTION		PAGE
1.0	Commissioner's Message	4
2.0	Key Issues	10
3.0	Role and Mandate	15
4.0	Access to Information Dispute Resolution	18
5.0	Privacy Complaint Investigations	32
6.0	Commissioner's Orders	42
7.0	Providing Advice	48
8.0	Informing the Public	51
9.0	Financial Statements	52

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Table of Figures

Figure		Page
1	Disposition of Requests for Review April 1, 2001 to March 31, 2002	21
2	Applicant Type — Requests for Review April 1, 2001 to March 31, 2002	22
3	Disposition of Requests for Review by Public Body April 1, 2001 to March 31, 2002	23
4	Grounds of Requests for Review by Public Body April 1, 2001 to March 31, 2002	24
5	Disposition of Access and Privacy Complaints April 1, 2001 and March 31, 2002	38
6	Disposition of Privacy and Access Complaints by Grounds April 1, 2002 and March 31, 2002	39
7	Access and Privacy Complaints by Public Body April 1, 2001 to March 31, 2002	40
8	Disposition of Access and Privacy Complaints by Public Body April 1 2001 to March 31, 2002	41
9	Disposition of Commissioner's Orders April 1, 2001 and March 31, 2002	44

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

1.0 Commissioner's Message

A shadow is cast over open and accountable government

The government has on many occasions affirmed its commitment to being – as is said in the New Era election platform – the "most open, accountable and democratic government in Canada." Given the pace and scope of change in this province, and the lack of a sizeable opposition in the Legislature, this goal is more significant than ever. Changes to government and severe budget reductions represent a threat to the access and privacy rights of all British Columbians.

More work, less money

There has been a lot of change in British Columbia over the last twelve months. More change is promised. Some public institutions have seen their funding substantially reduced, the role of government is under scrutiny, and new ways of delivering services are under serious consideration. All of these developments impact directly on the work of the Office of the Information and Privacy Commissioner ("OIPC").

Since my last annual report, the workload of the OIPC has increased considerably. Yet our funding has been cut by 10% in the 2002-2003 fiscal year and two further cuts are in the cards. The cuts were recommended in December 2001 in the report to the Legislative Assembly by the Select Standing Committee on Finance and Government Services, *Financial Review of the Statutory Officers of British Columbia*. The Committee has recommended cuts in the OIPC's funding of a further 10% in 2003-2004 and yet another 15% in 2004-2005. The total cuts would see the OIPC's budget – which had already been cut slightly in previous years – slashed from the 2001-2002 figure of $2,344,000 to $1,524,000 in 2004-2005, a decrease of $820,000.

To meet the first cut, I have eliminated three FTE positions, reduced our rented space by roughly 30%, and cut our budget for a number of important items (including legal services). I have already said publicly that the OIPC likely can weather this first cut without seriously affecting how we discharge of our regulatory functions. This is so even though we have been hit with cost increases for reasons beyond our control and even though we will likely see further increases in demand for the statutory appeal and complaint investigation functions we are legally required to provide.

Without belabouring what I said in the OIPC's 2002-2005 Service Plan, which I tabled in the Legislature in February, I remain gravely concerned that implementation of the further

recommended cuts will irreparably harm the OIPC's ability to perform its mandated functions and deliver services to British Columbians under the *Freedom of Information and Protection of Privacy Act* ("Act"). The cuts will, at the very least, mean the OIPC cannot address access appeals and privacy complaints in a timely fashion. At the extreme, it will not be possible to devote sufficient resources to deal with complex or contentious investigations or complaints.

Because there are so few Opposition members, and because of the rapid changes underway in government, this is not the time to hobble the OIPC, which is the independent oversight agency responsible for ensuring compliance with the access and privacy rights given to the public under the Act. Those rights are of fundamental importance in our democracy, as the Supreme Court of Canada affirmed in *Dagg* v. *Canada (Minister of Finance)* (1997):

> The overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry. ... Access laws operate on the premise that politically relevant information should be distributed as widely as reasonably possible. ... Rights to state-held information are designed to improve the workings of government; to make it more effective, responsible and accountable.

The government's move to revitalize the use of Select Standing Committees of the Legislative Assembly is a laudable step in the right direction. The government's stated commitment to making more information routinely available to the public is also commendable, although it is too early to tell how much success there has been, or will be, on this front. Still, the public's right of access to government information, enshrined in the Act, remains a key tool in any movement toward the greatest openness and accountability.

Various Cabinet members have repeated their commitment to such goals and to the workings of the Act. I have, however, heard rumblings from a few government MLAs about what they understand to be the large number of requests made by so-called 'frequent fliers' and the many requests they understand to be frivolous. As I have told these doubters, only the tiniest minority of requesters can be labeled nuisance requesters. Nor is it is a bad thing that political parties, the media, business groups and environmental groups regularly use the Act to gather information about what government is doing in the name of the public and with the taxpayers' money. It should be noted that the Liberal Party, while in Opposition, was appropriately an active

and vigorous user of the access rights under the Act. In any case, in the rare cases where a requester is abusing the right of access to information, the Act offers appropriate sanctions. Such abuse is rare. Legitimate use of the Act is the norm.

Now is the time to ensure that – as the Premier promised before the last election – the OIPC enjoys, to use the Premier's words, "stable funding", so we can ensure government remains open and accountable. I will therefore call on the Committee later this year to reverse its recommendation that further cuts be made to the OIPC's budget.

Before moving on, I will restate my ongoing support for the Committee's role in reviewing, and making recommendations on, the OIPC's budgets. The Committee may not always agree with what I do or say, publicly or otherwise, but I certainly respect and am grateful for their efforts and look forward to an open, ongoing dialogue.

Sharing services with other officers of the Legislature

Before last year's budget process before the Committee, the statutory officers of the Legislature decided to study whether sharing services could save money, thus allowing us to use the saved resources to serve the public. Early this year, the officers retained a management consultant to study shared services concepts, to examine the feasibility of shared services in light of the disparate mandates and operations of the various offices and to report back with identified options. Although it is not at all clear from the consultant's work that shared services will necessarily yield significant savings for the officers of the Legislature that remain interested in the idea, I am committed to examining the possibilities with the greatest care. I will proceed with shared services if they will allow us to devote our diminishing resources to delivering services to British Columbians.

Striving for OIPC transparency and accountability

As a statutory officer of the Legislature, my position is "independent" of government. This means I do not report to Cabinet or a Minister, but to the Legislature as a whole. I do not take direction, in the discharge of my statutory duties and functions, from a Cabinet Minister or a legislative committee; neither a Cabinet Minister nor a legislative committee can instruct me on how to rule on a particular matter. My role is to operate an independent and effective appeal system whereby citizens can have their privacy complaints and disputes over access to government records arbitrated by an agency outside of government.

Why is it important for the citizens of British Columbia to have access and privacy complaints reviewed by an independent agency? Independent review ensures government does not decide for itself what records the public should have access to. The Act sets strict rules defining the only circumstances in which public bodies may withhold information from a citizen. As Information and Privacy Commissioner, I have been given the responsibility to examine the records and rule on whether or not the rules have been properly applied.

To be "independent" does not, however, mean that I am not accountable for the taxpayer dollars the OIPC spends — to the contrary. Some of the ways in which the OIPC are accountable to the public include:

- The Commissioner's decisions in access to information appeals and privacy complaints can be judicially reviewed by the Supreme Court of British Columbia

- The Commissioner's administrative, but not operational, records are subject to the right of access under the Act and the Commissioner's decision on an access request for such records can be appealed to a judge of the Supreme Court of British Columbia

- The Commissioner is subject to the jurisdiction of the Ombudsman of British Columbia, to whom a complaint can be made under the Act

- A complaint can be made to the Speaker of the Legislative Assembly of British Columbia about the Commissioner or his office

- The Commissioner must appoint and terminate staff in accordance with the *Public Service Act*

- Although the *Budget Transparency and Accountability Act* does not apply to the Commissioner, I have committed to applying the service planning and budgeting standards under that Act as far as they can apply

- The annual budget of the OIPC is subject to review by, and the recommendations of, a Select Standing Committee of the Legislative Assembly of British Columbia

- The Auditor General of British Columbia has agreed to review the financial statements and activities of the OIPC for fiscal 2001-2002 and report the results, which I will deliver to the Legislative Assembly.

In line with my commitment to *Budget Transparency and Accountability Act* standards, I tabled a 2002-2005 Service Plan for the OIPC in the Legislature on February 19, 2002. That plan, which is found on the OIPC's website, scans the OIPC's operating environment, sets out performance measures and targets and provides a detailed budget breakdown for 2002-2003. I will report each year on the OIPC's success in meeting the planned targets and will revise the service plan as evolving circumstances require. As an aside, readers may recall that the OIPC's last annual report was, for the first time, a calendar-year report. Since the service plan reporting and budget activities must be undertaken on a fiscal-year basis, consistent with the new *Budget Transparency and Accountability Act*, I have decided it is necessary to switch back to a fiscal-year report, starting with this report.

Legislative amendments

On April 11, 2002, amendments to the Act came into force under the *Freedom of Information and Protection of Privacy Amendment Act, 2002*. Because the amending Act was given First Reading before the end of the fiscal year, I will say a few things about it here.

While it is fair to say many of the amendments are in the nature of welcome house-keeping changes, I will comment on three of the more important aspects of the changes. First, heeding the 1999 recommendations of the Special Committee of the Legislative Assembly to review the Act, the Legislature has given me more flexibility in discharging my appeal responsibilities under the Act. I can now, for the first time, delegate my order-making power in access appeals under the Act, bringing the British Columbia legislation into line with Ontario, Alberta and elsewhere in Canada. This will allow me to delegate decisions that do not involve new or complex issues, thus freeing me up to address more complex matters.

Second, the Act now gives me more flexibility to deal with those who are abusing their access rights under the Act, by allowing me to authorize a public body to ignore frivolous or vexatious requests. The Act has always given the Commissioner the authority to authorize a public body to ignore requests, but the test for when that power could be used was much stricter. On a related note, the Act now permits me to refuse to hold an inquiry for an access appeal, thus

allowing me to implement a fair, but more informal, method of disposing of frivolous appeals to the OIPC.

Third, the Act now requires all provincial government ministries to perform a privacy impact assessment ("PIA") for any policy, program or legislation that may impact privacy rights, and to deliver the PIA to the Corporate Privacy and Information Access Branch of the Ministry of Management Services. I applaud this progressive and ground-breaking provision. The PIA is a critical tool in assessing the privacy implications of e-government initiatives, shared service delivery and private sector delivery of services. All public bodies, not just government ministries, should undertake a PIA for any new or revised program or policy that may involve the collection, use or disclosure of personal information. A PIA is clearly an invaluable tool for identifying and addressing any privacy implications that may arise under the Act. In addition, since the Act's privacy provisions are the starting point, not the end-point, of good privacy practice, the PIA process should also address the broader policy question, 'Even if this proposal complies with the letter of the Act, are its privacy implications such that we should not proceed?'

The last point about the amendments relates to timelines under the Act. The Act used to refer to calendar days, but now defines a "day" to exclude Saturday, Sunday and any statutory holiday. This change materially increases, among other things, the statutory 30-day period within which a public body must respond to an access request. It also increases the length of any 30-day extension the public body may give itself. I would hope, given this increase in response times, that the OIPC will see fewer public body applications for a further extension of time under s. 10 of the Act. Those applications that we do receive will be dealt with bearing in mind the cumulative effective of the amended definition of "day".

David Loukidelis
Information and Privacy Commissioner
for British Columbia

2.0 Key Issues

My main message addresses issues that directly affect my office and its work. The following discussion touches on some significant access and privacy issues of the past year and coming years.

Video surveillance by police agencies

It is often tempting in our society to look to technology for solutions to complex social problems. A lot of attention this year has been paid to a technology that I fear, for the most part, offers false promises, while carrying risks. I refer to routine use by police of video surveillance in public spaces, an approach to law enforcement that is increasingly under consideration by Canadian police forces.

The police define their jobs in terms of crime prevention and public safety and, whenever possible, avail themselves of whatever tools are accessible in preventing crime and promoting public safety. My research in this area, however, leads unyieldingly to the conclusion the jury is still out with respect to the efficacy of video surveillance in the furtherance of these two objectives. The real impact these technologies have on our basic democratic rights, including our right to privacy, is often ignored, discounted, or rejected outright by many in the law enforcement community.

Some say there is no privacy in public spaces. If you have nothing to hide, they say, you should not fear being caught on police video. I strongly disagree, and concur with the thoughts of former Supreme Court of Canada Justice Gerard LaForest in his recent opinion given to the Federal Privacy Commissioner on this very point:

> Some citizens have said that they have nothing to hide and are comforted in the belief that video surveillance will permit the police to check the actions of malefactors. But this wholly mistakes the nature of a free society. It is not only criminals who are harmed by intrusions on liberty. In the absence of compelling justification, we should all be free to move about without fear of being systematically observed by agents of the state.

It is one thing to be observed casually by others as you go about your business in public, or even to be caught by chance in a photograph or home video as you

wander the streets. It is quite another thing, however, to be under the systematic, constant gaze of police video surveillance, regardless of what you are doing. Police video surveillance is just that – surveillance, not fortuitous, passing glances. As many have said, it is like having a police officer follow you around the town, two steps beside you, filming your every move on the streets. All of the captured images can be stored and retrieved forever, potentially for many purposes. The prospect of being followed and recorded in this way is not one most of us would really accept, regardless of what we might say off the cuff about having nothing to hide.

This is the reality in many urban centres in the United Kingdom. What is the purpose of all this filming and following? In the UK, the impetus to comprehensive video surveillance may have been terrorist bombing, although the government has never claimed that video surveillance was a real factor in stopping any bombings. The UK government nonetheless seems to have decided that video surveillance is worth investing in as a crime tool. The debate over its efficacy nonetheless rages on, though none of the many academic and police studies I have examined unequivocally claims that video surveillance reduces crime rates. The best view by far is that video surveillance merely displaces crime from one place to another, from one time to another, or from one kind of crime to another. Acknowledging the absence of clear proof of the effectiveness of video surveillance, the UK Home Office has embarked on a multi-year study of the efficacy of video surveillance, the results of which will not be ready until the autumn of 2004. Yet the UK continues to pour millions of pounds into video surveillance, while violent crime in London and other urban areas with video surveillance continues to rise. Why invest in a costly technology if it is not clear it works? Perhaps the answer is political. Video surveillance allows police and politicians to be seen to do something, and studies consistently show that people *feel* safer with video surveillance in their neighbourhood, even if they are not necessarily safer.

In Canada, crime rates – notably those for violent crimes – have been dropping steadily since 1991. British Columbia's crime rate dropped notably again in 2000. Yet many police forces are considering video surveillance as an alternative to more police on the streets and there is some public support for this. Is this because we *feel* less safe, even though crime is down?

If video surveillance makes people feel safer, and there is no privacy in public spaces anyway, why should anyone care about police surveillance of our everyday activities? There are two reasons. First is the potential for abuse,

beginning with misuse of video for prurient or improper uses. A more serious abuse would be use of video images for surveillance of individuals not suspected of any crime, including for political purposes. This concern is, given the present separation of police from government, highly unlikely, but it is an issue that cannot be ignored in the post-September 11 climate of increased state powers.

The second reason to be concerned about video surveillance is more philosophical, but nonetheless important. We should not underestimate the effect on our behaviour of being filmed all the time by cameras. It is inaccurate to suggest that all of our behaviour in public is not private. We often do things in a public place that are private in nature. Who hasn't stolen a kiss, tenderly embraced a loved one, shed a tear or had tense words with a parent, child or friend in some public place? If we know we are under constant police surveillance, most of us will be more inhibited, less spontaneous. Won't the result be that our actions in public will become masked or suppressed? I believe the answer is yes and I believe that this will have a real impact on how we relate to each other, as individuals and as members of our communities.

In June of 2000, the OIPC published *Guidelines for Video Surveillance of Public Spaces by Law Enforcement Agencies*. As these guidelines demonstrate, the OIPC acknowledges that video surveillance may be an effective law enforcement tool in specific circumstances. Even in such cases, however, a law enforcement agency faces a high bar in making the case, from a public policy perspective, that video surveillance is a cost-effective, useful tool in combating crime that should overcome the privacy and liberty interests that it can affect. I urge British Columbians to be extremely wary if they are told that their local police force wishes to use video surveillance because it will help in the fight against crime. Citizens should demand that, before their tax dollars are invested in expensive technology, the police make their case clearly and beyond doubt, and give assurances that privacy and liberty will not be inappropriately affected by video surveillance.

Delays in responding to access requests

At the risk of being thought of – wrongly – as someone who cries wolf, I must again express concern about delays in responding to access requests. Some are struggling to respond in time, as required by the Act, due to inadequate resources.

Concern about adequate resources is heightened, of course, by the cuts in ministry budgets announced last year. Indications are that the access and privacy staff of most ministries will not be spared, even though ministries have a legal duty to respond in the time required by the Act. To the extent staff remain on the job, some will be bumped by more senior staff, who often will not have the necessary extensive training and experience in dealing with the Act. In combination, the reduced staffing levels, and inexperience of new staff, are likely to cause further delays and maybe affect the quality of decisions, in the latter case in the short term at least.

I have urged various deputy ministers not to slash their access and privacy staff, especially in those ministries with a high proportion of individual requesters, who are seeking their own personal information. I have urged them to regard their access and privacy programs as services delivered directly to British Columbians and not to reduce those services if at all possible. In saying this, however, I have acknowledged that cuts in funding have generally been across the board within ministries. Still, this is a situation that the OIPC will be monitoring, although the only real solution is for program funding to be preserved ministry-by-ministry and, in some cases, increased to deal with significant increases in requests.

There is, again this year, a ray of light in all of this. Two ministries that have long struggled with significant backlogs of access requests have finally eliminated their backlogs. The Ministry of Children and Family Development has, to its great credit, reduced what was once a very large case backlog to nothing. Similarly, the Ministry of Human Resources has all but defeated its long-standing backlog, with a small number of cases yet to go. Past and present deputy ministers and access and privacy staff, are to be congratulated on their success in slaying the monster.

Alternative Service Delivery

The Act gives the public a right of access to records in the custody and control of public bodies. It also sets rules around the collection, use and disclosure of personal information collected by public bodies. Will the privacy and access rights of citizens be recognized and protected in the privatization of services formerly delivered by government? Providing government services through alternative service delivery raises special challenges to accountability, transparency and the protection of privacy.

With respect to privacy protection, the government must ensure that all alternative service delivery mechanisms are structured, by statute or by contract, in such a way to ensure that British Columbians' personal information is appropriately handled by private sector service providers. In related initiatives, in October of last year, the OIPC published *Guidelines for the Audit of Personal Information Systems* containing personal information. In November of last year, we published *Guidelines for Data Services Contracts* that involve personal information. In the coming year we will continue to keep abreast of the privacy implications of alternative service delivery initiatives, including public private partnerships, and will comment on the privacy implications of such initiatives. We will also address the access to information implications of P3s and other alternative service delivery mechanisms, with a view to offering guidelines along the lines of those just described.

3.0 Role and Mandate

British Columbia's *Freedom of Information and Protection of Privacy Act* came into force on October 4, 1993. It helps citizens hold government bodies accountable by giving the public a right of access to records and limiting the circumstances in which requests for records may be refused. The Act also protects the privacy of citizens by preventing the unauthorized collection, use or disclosure of personal information by public bodies.

Some suggest that the goals of the Act — freedom of information and protection of privacy — conflict. In fact, the two goals are compatible. The right of access to information gives the public the ability to request records relating to the decisions, operations, administration and performance of government. The underlying premise is that citizens are best equipped to hold government accountable and better able to participate in the democratic process when they have timely access to relevant information. This is reflected in the Act's purposes, which are set out in s. 2(1). That section affirms that one of the Act's main objectives is to make public bodies more accountable to the public. This is why the right of access to information is, as s. 2(1) confirms, given "to the public". This goal of access to information laws was affirmed by the Supreme Court of Canada's decision in *Dagg*, as stated earlier in the Commissioner's Message.

The Act's privacy provisions implement internationally-recognized limits on government's ability to collect, use and disclose individuals' personal information in the delivery of public services. The Act's rules hold public bodies accountable for their actions as they affect our personal privacy by limiting how public bodies can collect, use and disclose personal information, and how citizens can get access to their own personal information.

The Act:

- Establishes a set of rules specifying limited exceptions to the rights of access
- Requires public bodies to make every reasonable effort to assist applicants and to respond to access requests openly, accurately and without delay
- Requires public bodies to respond to access requests within legislated timeframes

- Requires a public body to account for information it withholds in response to a request for records
- Establishes strict standards around when and how public bodies may collect, use and disclose personal information
- Provides for independent review and oversight of decisions and practices of public bodies concerning privacy and access rights

The roughly 2,000 public bodies covered by the Act include ministries, Crown corporations, government agencies, boards and commissions, school districts, colleges, universities, self-governing professions, municipalities, municipal police forces, health authorities, hospitals, regional districts and library boards.

Part 4 of the Act establishes the Office of the Information and Privacy Commissioner. The Information and Privacy Commissioner, David Loukidelis, is an independent officer of the Legislature. The Commissioner is appointed for a six-year, non-renewable term, and reports to the Legislative Assembly of British Columbia. The mandate of the Office is to provide an independent review of government decisions that involve access and privacy rights.

The Commissioner is generally responsible for monitoring how the Act is administered to ensure that its purposes are achieved. Under section 42 of the Act, the Commissioner has the power to:

- Investigate, mediate and resolve appeals concerning access to information disputes
- Investigate and resolve privacy complaints
- Conduct research into anything affecting access and privacy rights
- Comment on the access and privacy implications of proposed legislation, programs or policies
- Comment on the privacy implications of new technologies and/or data matching schemes
- Educate the public about their access and privacy rights

The Commissioner has delegated some of these powers to his staff, who conduct investigations, mediate disputes, engage in public education activities and work with public bodies to ensure access and privacy rights are factored into the decision making process.

4.0 Access to Information Dispute Resolution

One of the cornerstones of the *Freedom of Information and Protection of Privacy Act* is the right of citizens to appeal to an oversight body, independent of government, all access to information decisions made by public bodies. This is the role of the Commissioner and his office. A request for review can be filed regarding the refusal by a public body to disclose information, a failure to respond to access requests, refusal to correct personal information, the adequacy of a search for requested records, the appropriateness of a fee or any other action or decision of a public body in responding to an access request.

Section 55 of the Act allows the Commissioner to authorize mediation for any matter under review. The OIPC has a long and remarkable history of mediating access appeals, and last year resolved fully 90% of access appeals through mediation. The mediation process involves a Portfolio Officer reviewing the records, discussing with all parties the circumstances of the review and attempting to facilitate, through various means, either a full or partial settlement of the issues under review. The Portfolio Officer is not an advocate of either the applicant or the public body. The role of the Portfolio Officer is to ensure that the applicant has received all the information to which he or she is legally entitled, taking into account the circumstances of the case, the applicable sections of the Act and previous decisions by the Commissioner relevant to the issues.

The Act gives the OIPC 90 days from the day the case is opened to resolve the matter. The first 68 days is the mediation phase. After that time, if a settlement cannot be achieved, the matter may proceed to a formal inquiry before the Commissioner.

Mediation may result in any or all of the following outcomes:

- Further information is released to the applicant
- A reduction in the number of records in dispute
- Confirmation or reduction of a fee
- Additional records responsive to the request are located

- Clarification of outstanding issues that cannot be settled by mediation
- Referral to another agency for resolution of the issue (*e.g.*, the Ombudsman)

From April 1, 2001 to March 31, 2002, the Office successfully resolved, without a formal inquiry, 842 of the 923 requests for review filed during that period.

Many different individuals or organizations rely on the Act to obtain information. They include individuals, the media, political parties, individual businesses, business groups, unions and labour organizations, the legal profession, elected officials, First Nations, environmental groups and community organizations. One of the questions we are most frequently asked is, "Who most frequently requests the services of the OIPC?" Fully 73% of all requests for review are made by individuals seeking information affecting their own interests.

Another question that is commonly asked is, "Which public bodies are most frequently the subject of OIPC reviews?" Consistent with previous years, decisions by ICBC, the Ministry of Attorney General and Ministry of Solicitor General together, the Workers' Compensation Board and the Ministry for Children and Family Development are the subject of the most appeals. This is not surprising, as these public bodies also receive high numbers of requests for information and collect, use and disclose more personal information than many other public bodies.

The Act creates a set of rules that public bodies must respect when responding to access requests. The Act ensures access requests are promptly answered by requiring public bodies to respond within 30 days (unless the time is extended as permitted in the Act). The Act also creates a duty for public bodies to respond openly, accurately and without delay, and sets rules on the type and amount of fees that may be charged for responding to a request.

Anyone who believes a public body has failed to abide by these rules or perform a duty required by the Act may complain to the OIPC. Access complaints relate to a variety of issues, including:

- The appropriateness of a fee
- Whether a fee should be excused in whole or in part in the public interest
- Whether a public body was justified in taking a time extension to respond to an access request
- Delays in responding to an access request

The procedure for investigating access complaints is very similar to the procedure for investigating privacy complaints. A Portfolio Officer is assigned to the case. She or he examines all the circumstances surrounding the complaint. If the complaint is substantiated, the Portfolio Officer may make recommendations to the public body that address issues affecting access rights. In rare circumstances, the complaint may be dealt with directly by the Commissioner.

From April 1, 2001 to March 31, 2002, the OIPC closed 40 access complaints. Of those, 25 were complaints that a public body had failed to perform a duty, for example to respond openly, accurately and without delay. Of those, 14 were either fully or partially substantiated and 11 were found to be unsubstantiated.

Figure 1:

Disposition of Requests for Review
April 1, 2001 to March 31, 2002

GROUNDS	MEDIATED	ORDER	DISCONTINUED[2]	TOTAL
Access:				
Denied Access	130	17	2	149
Partial Access	334	29	7	370
Adequacy of Search	124	10	1	135
Correction Request	4	4	1	9
Deemed Refusal	162	4	0	166
Duty to Assist	16	6	0	22
Fees	28	5	0	33
Scope of Act	8	1	0	9
Third-Party Request for Review	20	5	1	26
Time Extensions	3	0	0	3
Other	1	0	0	1
Total	**830**	**81**	**12**	**923**

[2] "Discontinued" indicates those requests for review that were abandoned or withdrawn by the applicant.

Figure 2:

Applicant Type[3] — Requests for Review
April 1, 2001 to March 31, 2002

TYPE OF APPLICANT	REQUESTS FOR REVIEW	PERCENTAGE OF TOTAL
Individual	682	73.8%
Organization[4]	59	6.4%
Commercial	59	6.4%
Media	44	4.8%
Lawyer	31	3.4%
Special Interest Group[5]	23	2.5%
MLA	22	2.4%
First Nations	3	0.3%
Total	**923**	**100.0%**

[3] This is a difficult statistic to track accurately, since the Act does not require applicants to identify themselves as belonging to a particular group. When applicants do identify their affiliation, the request for review is categorized accordingly. If an applicant does not identify any affiliation, he or she is categorized as an individual requester. This may render the category of "Individual" slightly higher than is actually the case.

[4] "Organization" includes unions, associations, societies and non-commercial organizations.

[5] "Interest Groups" include environmental, wildlife and human rights groups.

Figure 3:

Disposition of Requests for Review by Public Body
April 1, 2001 to March 31, 2002

PUBLIC BODY	REQUESTS FOR REVIEW	MEDIATED	DISCONTINUED	ORDER
Insurance Corporation of BC	147	133	0	14
Attorney General & Public Safety and Solicitor General[6]	88	82	0	6
Workers' Compensation Board	52	45	2	5
Children and Family Development[7]	45	39	3	3
Vancouver Police Department	41	39	1	1
Finance[8]	23	22	0	1
Health Services/ Planning[9]	23	23	0	0
University of British Columbia	21	9	0	12
Forests	20	19	0	1
Water, Land and Air Protection and Sustainable Resource Management[10]	20	15	1	4

[6]Formerly the Ministry of Attorney General
[7]Formerly the Ministry for Children and Families
[8]Formerly the Ministry of Finance and Corporate Relations
[9]Formerly the Ministry of Health
[10]Formerly the Ministry of Environment, Lands and Parks

Figure 4:

Grounds of Requests for Review by Public Body
April 1, 2001 to March 31, 2002

	TOTAL	ADEQUATE SEARCH	CORRECTION REQUEST	DEEMED REFUSAL	DENIED ACCESS	DUTY TO ASSIST	FEES	PARTIAL ACCESS	SCOPE OF THE ACT	THIRD PARTY	TIME EXTENSION	OTHER
Insurance Corporation of BC	147	7	0	17	6	3	1	112	0	0	1	0
Attorney General & Public Safety and Solicitor General	89	14	1	25	23	1	1	23	0	1	0	0
Workers' Compensation Board	52	13	1	10	8	1	1	16	1	1	0	0
Children and Family Development	45	5	3	6	6	2	0	22	0	0	0	1
Vancouver Police Department	41	13	0	0	8	0	2	16	2	0	0	0
Finance	23	1	0	13	0	1	1	7	0	0	0	0
Health Services & Health Planning	23	4	0	9	4	0	0	6	0	0	0	0
University of British Columbia	21	4	0	1	5	0	0	8	0	3	0	0
Forests	20	2	0	9	2	1	1	5	0	0	0	0
Water, Land and Air Protection & Sustainable Resource Management	20	1	0	4	1	0	2	6	1	5	0	0

Examples of Mediated Access to Information Disputes

The following examples of successfully mediated access to information appeals illustrate the range of issues brought to the OIPC in 2001-2002.

The adequacy of a search for records by the Ministry of Attorney General

The applicant applied for a firearms license, the processing of which is carried out by staff of the Security Programs Division of the Ministry of Attorney General. Upon the granting of the license, a restrictive condition was attached without an explanation as to why. The Ministry kept no records of its deliberative process; it simply viewed online whatever information about the applicant was contained in CPIC (Canadian Police Information Centre) records and imposed any conditions on the license its staff deemed appropriate.

The Portfolio Officer explained to the applicant that the Act applies only to records that exist, and if, as in this case, there are no records, the OIPC cannot do anything. However, the practice of providing reasons for decisions that affect individuals is a matter of administrative fairness. The Portfolio Officer explained to the applicant the option of contacting the Ombudsman's Office for assistance in this respect.

A decision by the Ministry of Water, Land and Air Protection to withhold third-party business information

The applicant requested site surveys provided by a major oil company to the Ministry as part of a statutory obligation to report on the state of contaminated land. The applicant was a law firm representing the owner of a shopping mall in a lawsuit against the oil company for damage caused by migrating sub-surface pollutants. The oil company declined to authorize release, citing s. 21. That section requires a public body to withhold information the release of which could harm the business interests of a third party – in this case, the oil company.

In the mediation process, the Portfolio Officer noted that all three parts of s. 21 must be satisfied for the legal protection to apply. First, the information had to be commercial, technical or scientific information of the third party. Second, that

information must have been supplied in confidence to the public body. Third, one of the various harms listed in the section must reasonably be expected to occur if the disputed information were released. The Portfolio Officer suggested that the oil company would have a difficult task to convince the Commissioner that the information was submitted in confidence or that the harms set out in s. 21 were likely to accrue. The oil company subsequently agreed to full disclosure of the requested reports.

A Crown corporation decision to withhold information that would harm its financial or economic interests

The applicant, a retired civil engineer, was a homeowner who alleged that Skytrain construction activities, especially blasting, had caused extensive structural and cosmetic damage to his home. In an effort to establish this, he sought full disclosure of Skytrain construction engineering and soil analysis reports. The public body complied with the request, but withheld comments from an independent adjuster's report as well as a variety of records relating to construction engineering practices, soil conditions encountered during construction and other technical drawings. This information was withheld under s. 17, which allows a public body to withhold information if disclosure of that information would harm the public body's financial interests. The Portfolio Officer contended that the information withheld fell short of meeting the test of a reasonable expectation of harm attributable to the release of the information. The public body reconsidered its position and decided to release all of the information to the homeowner.

A School District decision to withhold third-party personal information

A parent made a request under the Act to a school district for a copy of an investigation report concerning her son's teacher. The school district had conducted the investigation after the parent complained that the teacher's actions toward her son amounted to emotional and physical abuse.

The school district disclosed the report to the parent, but not before severing a significant amount of personal information from it. During mediation, the applicant acknowledged that the school district correctly severed the information she was particularly interested in seeing. It was still possible, however, for the school district to provide information to the applicant in a way that

satisfied her concerns and preserved the privacy of third parties. The applicant's reason for making the request was so she could reassure her son that he had done the right thing. She felt it was important for him to believe he was right to voice his concerns and that it was worth it for him to experience the intimidation he felt during the school district's investigation.

The school district sent a letter to the student stating in principle that it was appropriate for him to tell his mother that he was worried and that the information he gave during the investigation was valuable. The effect of this was to satisfy the applicant's purpose for making the request while maintaining the privacy of the third parties involved.

A decision by the Ministry of Skills Development and Labour to withhold information not covered by the Act

The applicant had an appeal hearing before the Medical Review Panel (MRP) of the Workers' Compensation Board (WCB) and later requested copies of notes taken by the doctors on his MRP. The Ministry responded by denying access to the MRP notes on the grounds that they were excluded under s. 3(1)(b) of the Act. That section provides that the Act does not apply to "a personal note, communication or draft decision of a person who is acting in a judicial or quasi-judicial capacity."

The records in question were notes taken by the doctor who chaired the MRP that heard the applicant's case. The Portfolio Officer agreed that the doctor's notes fell under s. 3(1)(b). She then compared the notes to the medical decision documents – copies of which the applicant received as part of his appeal – and found that the two contained much the same information. In this light, the Portfolio Officer asked the Ministry to consult with the MRP, and the chair of the applicant's panel, to find out if they would agree to disclose the notes. Both maintained that s. 3(1)(b) applied to the records but decided that, in this case, they had no objection to their disclosure. The Ministry therefore sent the applicant a copy of the notes and this resolved the request for review.

A decision by the Workers' Compensation Board to withhold law enforcement information

The applicant requested all his records from the WCB, which he received. He later requested disclosure of any records that post-dated his first request, in

particular any investigation records related to surveillance of his activities. The WCB provided some updated records, but refused to confirm or deny the existence of records under section 8(2) of the Act. The applicant requested a review of this decision, stating that he had seen an investigator parked outside his house and that this investigator had been filming him.

The WCB subsequently changed its decision, to a refusal to provide access to investigation records under s. 15(1) of the Act, which allows a public body to withhold information if its disclosure would harm a law enforcement matter. The Portfolio Officer's inquiries revealed that the investigation was now finished. At the Portfolio Officer's recommendation, the WCB disclosed almost all of the records it had withheld, except one item which it continued to withhold on the grounds that disclosure would reveal a confidential source of law enforcement information. Further discussions ensued, including consultation with the individual whose identity the WCB was protecting. With the consent of that individual, the WCB agreed to disclose the remaining withheld information to the applicant.

A decision by an improvement district to refuse to provide records to a board member

The applicant, an elected member of the board of an improvement district constituted under the *Local Government Act*, was denied access to information she requested on the grounds that it was subject to solicitor client privilege. The other members of the board were permitted access to the same records. During mediation, the board agreed that the client in question was in fact the entire board, not just some members of the board. The records were released to the applicant.

In an effort to establish ground rules and improve the overall functioning of the Board, all members of the Board signed an agreement that clarified access procedures, circumstances in which records would be created and the process by which privilege could be waived.

A review of a fee levied by a Regional District

In response to a request for records, a regional district levied two fees amounting to just over $1,000. The applicant asked the OIPC to review whether or not the fee was appropriate. During mediation it became clear that that the request was

very broad and the regional district estimated it would take a minimum of 14 hours just to locate the records. During mediation, the regional district offered to create a list of the types of records that might be responsive to the request. The applicant accepted this proposal and used this list to narrow the request, which saved both the applicant and the regional district time and money. The regional district also offered to meet with the applicant on a face-to-face basis to discuss his original concerns that precipitated the access request.

A decision by a municipality to withhold solicitor-client privileged information

The applicant, representing a community group, made a request for records relating to a residential redevelopment. The redevelopment had taken place 18 years earlier. In response, the municipality provided some records, but withheld others on the ground that they were protected by solicitor client privilege under s. 14. During mediation, the Portfolio Officer encouraged the municipality to reconsider its decision, on the ground that the information was factual in nature, was uncontroversial and had mostly been disclosed in 1984 in newspaper articles and through public announcements at the time. In the spirit of open government, the municipality decided to release the records to the applicant.

A School District decision to withhold third-party personal information

A parent, whose son had been involved in an incident during a school field trip, requested records regarding this and another incident involving the son and his teacher. Initially, the school district disclosed the investigation report and other records regarding both incidents, but withheld personal information about other students, parents, teachers and other school district employees. It did so because it believed disclosure of this information would unreasonably invade third-party privacy.

Through mediation, the school district agreed to disclose more information about the parent and her son (intertwined with others' personal information) as well as information concerning various employees that was really information about their functions as employees. The school district continued to withhold the principal's comments about the teacher's performance, as well as the teacher's personal opinions about issues unrelated to the parent or her son. As a result, the parent received most of the information in the records and accepted this as a mediated resolution to her request for review.

A Ministry of Forests decision to withhold copyrighted information

An environmental group applied to the Ministry of Forests for a digital map of all forest development plans, including amendments for the 2000 operating season. The Ministry responded by stating the applicant should request the information directly from the licensees. In part, the Ministry took this approach because of copyright concerns.

Forest companies are required by the *Forest Practices Code* to submit Forest Development Plans to the Ministry. The *Code* specifies that the plans must contain certain information, including the location of cutblocks and roads.

During mediation, the Portfolio Officer established for the Ministry that the federal *Copyright Act* expressly states that it is not an infringement of copyright to disclose information through an access to information statute. The Ministry reconsidered its original decision and decided to give the applicant full access to the records.

A hospital's decision to withhold information from the Public Trustee

A lawyer for the Public Trustee requested information about a specific individual from a hospital. The Public Trustee was acting on behalf of the individual to pursue a claim for compensation related to Hepatitis C. The hospital required the Public Trustee to provide documentation of the Public Trustee's appointment, as committee of the individual, rather than its appointment as committee of the individual's estate before it would respond. Usually the committee of the person makes decisions about the physical person, while the committee of the estate makes the financial decisions. As a result, the request was denied and the Public Trustee sought a review of the hospital's decision.

During mediation, a discussion ensued about the current state of the law in British Columbia with respect to appointed committees. The conclusion was that the committee of the estate may act as litigation guardian in matters that go beyond property or financial matters. In addition, the Portfolio Officer reviewed the hospital's policies and suggested that those policies did not support the position the hospital had taken. The policy of the regional health authority did make it clear that the Public Trustee, if acting in a matter of litigation, could have access to the medical information.

The Portfolio Officer asked the hospital to process the request under the Freedom of Information and Protection of Privacy Regulation, made under the Act. The Hospital then released the information to the Public Trustee. the Portfolio Officer also suggested the hospital should amend its policy to address the specific issue of access to information by the committee of estate acting as litigation guardian.

5.0 Privacy Complaint Investigations

The term "privacy" is not actually defined in the Act. Privacy means different things to different people. To some, privacy means the "right to be left alone". To others, it means anonymity. Still others believe it means the right to be unobserved. Under the Act, privacy means maximizing, wherever possible and to the extent that is reasonable, a citizen's control over the collection, use and disclosure of his or her personal information.

To that end, the Act contains a set of internationally recognized rules – called "fair information practices" – that govern the collection, use and disclosure of personal information by public bodies. Collectively, those rules implement the basic premise that public bodies must be appropriately restrained, transparent and vigilant in the management of personal information collected in the delivery of public services.

The Act requires public bodies to adhere to standards respecting:

- The purposes for which personal information may be collected, used and disclosed
- How personal information is to be collected
- What a public body must tell an individual when collecting her or his personal information
- The duty to take reasonable steps to ensure personal information is accurate
- The duty to take reasonable steps to protect personal information from unauthorized access, use and disclosure
- The circumstances in which personal information may be used and disclosed
- How long personal information must be retained

Sections 42(2) and 52 of the Act authorize the Commissioner to receive and investigate complaints about a public body's compliance with the Act. Anyone who believes his or her personal information has been inappropriately collected,

used or disclosed by a public body can ask the Commissioner to investigate the alleged breach. An individual can also complain about a public body's alleged failure to properly secure personal information against unauthorized use, disclosure or destruction or about the public body's refusal to correct personal information. The Commissioner also has the authority to investigate such matters even if no complaint is received.

Most complaints are received in writing. They are then assigned to a Portfolio Officer to investigate. The circumstances surrounding the complaint will be carefully examined and a determination will be made as to whether the complaint has merit. If the complaint is substantiated, the Portfolio Officer will work with the public body to ensure remedial steps are taken to correct the problem and reduce the risk of re-occurrence. In addressing the problem, the public body may have to change the way it uses, discloses, collects or stores personal information, implement training programs or change policies and procedures.

If the matter under investigation is of a systemic nature or one that affects a significant number of people, the findings of the investigation may be issued publicly. The OIPC issued two such public findings last year, one of which is mentioned below. In very rare cases, the complaint may be referred to the Commissioner, who may conduct an inquiry into the matter.

Between April 1, 2002 and March 31, 2002, the OIPC investigated 81 privacy complaints. Of those, 24 were substantiated, 51 unsubstantiated, 4 discontinued and 2 were the subject of Investigation Reports. Most of the privacy complaints concerned allegations that a public body inappropriately disclosed personal information.

Examples of Privacy Complaint Investigations

The following summaries are examples of some of the privacy complaints the OIPC investigated and resolved during 2001-2002.

Exchange of employee information between different employers

An individual, who was an on-call employee in two health regions, complained that one region had violated her privacy by disclosing her hours of work to the second region. The individual had been booked to work a specific shift in the

first region, but cancelled the shift by informing the region that she was ill. The first region later learned that the individual might have actually worked at the second region during this time period. If this was the case, the individual might have violated her employment agreement with the first region. It thus requested and received from the second region a copy of the individual's hours of work for the time in question.

The Portfolio Officer's review determined that the disclosure was appropriate, since the first region was asking for the information for a purpose consistent with the purpose for which it was originally collected. The complaint was thus found to be unsubstantiated. The review highlighted that it is permissible, in certain circumstances, for employers to exchange employee information.

Use of a hospital employee's health information

A hospital worker complained that her privacy had been violated. She alleged that hospital management had disclosed her medical information at a meeting where union representatives were present. She also complained that the use of her medical information from her patient chart for employment-related purposes was inappropriate.

A meeting had been scheduled with management and the worker to discuss employment-related concerns. The union was to be present at the meeting, at the worker's request. In preparation for the meeting, management staff reviewed a series of patient charts. Unexpectedly, one of the charts pertained to the worker as a patient in the hospital. Management determined that the information in the chart raised questions about the worker's fitness for the job. Management decided to raise this with the worker at the meeting. The issue arising from the patient chart was discussed at the meeting and the records disclosed to the worker and the union representatives.

The Portfolio Officer's review of the complaint determined that, while it was appropriate for the hospital to discuss its concerns with the employee, the individual's privacy had been violated as a result of the disclosure of her medical information, without her consent, to the union representatives present. The Portfolio Officer recommended that, if such a situation arose again, steps should be taken before any meeting to inform staff that their medical information would be disclosed.

The hospital conducted a review of its own and came to the same conclusion. It apologized to the worker.

Ministry's disclosure of employee's medical information to Ministry managers

The complainant alleged that her employer had written a letter to her doctor and had sent copies of the letter to managers in her Ministry. She objected to the fact that the letter mentioned of one of her medical symptoms. She felt that mention of this symptom in a letter copied to the managers who did not need to know the information was an embarrassment and a violation of her privacy.

The Ministry said that this employee had been engaged in a long-running labour dispute with management. Two of the three managers who had received copies of the letter had previous involvement in the employee's claims for various benefits and were already aware of the symptom information. The Ministry also argued that managers to whom the information had been disclosed needed to be kept up to date on developments in the employee's case. Other employees had similar disputes, it said, and managers had received copies of similar correspondence in those cases as well.

The OIPC recommended that the Ministry develop ways of limiting disclosure of employee medical information to staff who were involved in dealing with an employee's claims. The OIPC also acknowledged that senior staff need to be kept up-to-date on controversial employee matters, but recommended that the Ministry develop methods of briefing those senior managers without disclosing employee medical information. The Ministry accepted the OIPC's recommendations and agreed to implement the necessary changes to its procedures.

Inappropriate physical security for personal information

The complainant expressed concerns about storage and security of student loan applications by the Ministry. The complainant said that, for example, many loan applications were being left on desks overnight.

The Portfolio Officer determined that some of complainant's concerns were substantiated, in that staff left files containing loan applications on their desks overnight and that the file storage area was not fully enclosed. Outside cleaning staff also had unsupervised access to the Ministry's student loan office at night. The OIPC recommended that the Ministry provide better physical

security for its paper files and the Ministry accepted this recommendation. First, it arranged for staff to store files overnight in lockable filing cabinets. It also enclosed the file room and installed lockable doors.

Employee inappropriately accessing and disclosing personal information for personal reasons

A woman complained that a Ministry employee inappropriately accessed her name through the judicial system database and then disclosed the information to mutual acquaintances. The employee admitted to inappropriately accessing and disclosing the information.

During the investigation, the employee's supervisor argued that the fact that the information in the court database was "public" was a mitigating factor. The OIPC acknowledged that information in a court file is available to the public, meaning anyone who makes the effort to attend the relevant court registry can, in the absence of a ban on publication, review the file. However, the OIPC also took the view that this does not translate into Ministry employees being free to access information on databases for which they have no operational need and does not confer the right to disclose information so accessed outside of the workplace.

The Ministry was very concerned about the incident and, upon being contacted by the OIPC, immediately conducted its own internal investigation. The Ministry determined that the employee's access was contrary to the terms and conditions under which access to the court system is granted and appropriate action was taken. As a result of this complaint, Ministry employees were reminded of the rules regarding the use and disclosure of personal information.

Data services contract between the Vancouver Hospital and Health Sciences Centre and Telus

This investigation dealt with the BC Nurses' Union (BCNU) complaint regarding a series of contracts entered into in 1996 by Telus and the Vancouver Hospital and Heaith Sciences Centre (VHHSC) to allow the VHHSC to use the LastWord system as its electronic medical records system. The BCNU concern was that the language of the contracts created the potential for

patient information in the custody or control of the VHHSC to be inappropriately accessed, used or disclosed. The BCNU was further concerned that the VHHSC would have few remedies if such a violation occurred.

The OIPC concluded that, while contract wording could legitimately give rise to privacy concerns on the part of someone unfamiliar with the history behind the contracts and their implementation, the day-to-day security arrangements in place between VHHSC and Telus provided adequate safeguards.

The resulting publicly-released investigation report provided a number of recommendations specific to the contracts under review, but which the OIPC believes public bodies should consider when entering in to similar contracts in the future. Some of the OIPC's key recommendations are as follows:

- Privacy Impact Assessments should be completed as part of the process of developing any contracts involving personal information
- The contract should clearly spell out that the public body is responsible for, and controls, personal information subject to the contract
- The contract should require the contractor, and any subcontractors, to comply with the Act
- The contract should outline the specific situations whereby the contractor or any subcontractors would require access to personal information
- The contract should include a schedule of regular and systematic audits of the contractor's and any subcontractor's compliance with the privacy provisions of the contract

Figure 5:

Disposition of Access and Privacy Complaints
April 1, 2001 and March 31, 2002

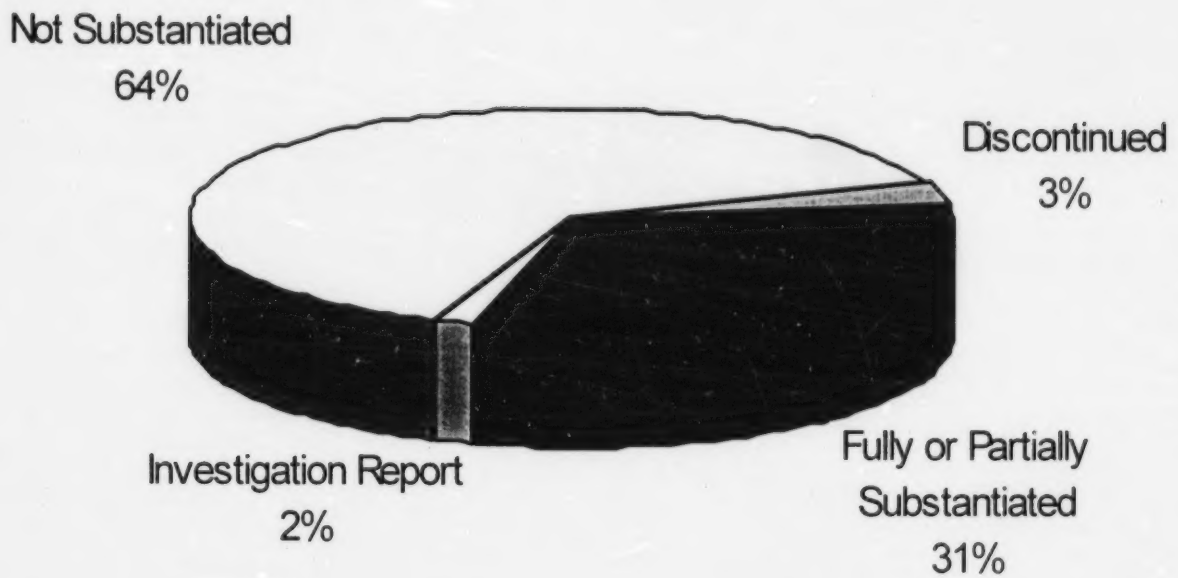


Figure 6:

Disposition of Privacy and Access Complaints by Grounds
April 1, 2001 to March 31, 2002

GROUNDS[11]	FULLY OR PARTIALLY SUBSTANTI-ATED	DISCONTINUED[12]	UNSUSTANTIATED	INVESTIGATION REPORT ISSUED
Time Extension	0	0	15	0
Failure to Perform a Duty	14	0	11	0
Inappropriate Collection	9	1	17	1
Inappropriate Disclosure	13	3	33	0
Inappropriate Use	2	0	1	1
Total	**38**	**4**	**77**	**2**

[11] Since many complaints and investigations involve more than one issue, they have been categorized by their predominant grounds only.
[12] "Discontinued" indicates those complaints that were abandoned or withdrawn

Figure 7:

Access and Privacy Complaints by Public Body
April 1, 2001 to March 31, 2002

PUBLIC BODY	COLLECTION	DISCLOSURE	DUTY	EXTEND	USE	TOTAL
Attorney General & Public Safety and Solicitor General[12]	6	6	1	5	1	19
Insurance Corporation of BC	1	6	2	0	0	9
Children and Family Development[13]	2	4	0	0	0	6
Human Resources[14]	0	4	2	0	0	6
Workers' Compensation Board	1	4	0	1	0	6

[12]Formerly the Ministry of Attorney General
[13]Formerly the Ministry for Children and Families
[14]Formerly the Ministry of Social Development and Economic Security

Figure 8:

Disposition of Access and Privacy Complaints By Public Body April 1, 2001 to March 31, 2002

PUBLIC BODY	FULLY OR PARTIALLY SUB-STANTIATED	NOT SUBSTANTIATED	DISCONTINUED	INVESTIGATION REPORT ISSUED
Attorney General & Public Safety and Solicitor General[15]	2	15	2	0
Insurance Corporation of BC	2	7	0	0
Children and Family Development[16]	2	4	0	0
Human Resources[17]	1	5	0	0
Workers' Compensation Board	1	4	1	0

[15]Formerly the Ministry of Attorney General
[16]Formerly the Ministry for Children and Families
[17]Formerly the Ministry for Social Development and Economic Security

6.0 Commissioner's Orders

In 2001-2002 the OIPC mediated a settlement in 90% of all access appeals. The rest were dealt with through a formal inquiry by the Commissioner under Part 5 of the Act. The Commissioner has the power to decide all questions of fact and law that arise during the inquiry and dispose of the matter by issuing an order under s. 58.

Before conducting an inquiry, the Commissioner is not involved in any way in the mediation process. This is to ensure that, if the matter proceeds to an inquiry, the Commissioner is unbiased by any previous involvement.

An inquiry may be conducted in person (oral inquiry) or through written submissions (written inquiry). The Commissioner determines whether or not an inquiry will proceed on an oral or written basis. Almost all inquiries are done in writing. In a written inquiry, both parties provide submissions to the Commissioner. The submissions are exchanged and both parties are permitted a response. If sensitive material is under review or must be discussed in detail, all or part of that portion of the submission may be submitted to the Commissioner *in camera*, which means, in effect, for the Commissioner's eyes only.

After the conclusion of an inquiry, the Commissioner will issue an order, which becomes a public document. In an order, the Commissioner may do any one or a combination of the following:

- Require the public body to give the applicant access to all or part of the record
- Confirm the decision of the public body or require the public body to reconsider it
- Require the public body to refuse access to all or part of the records
- Require that a duty imposed by the Act be performed
- Confirm or reduce the extension of a time limit for responding to a request

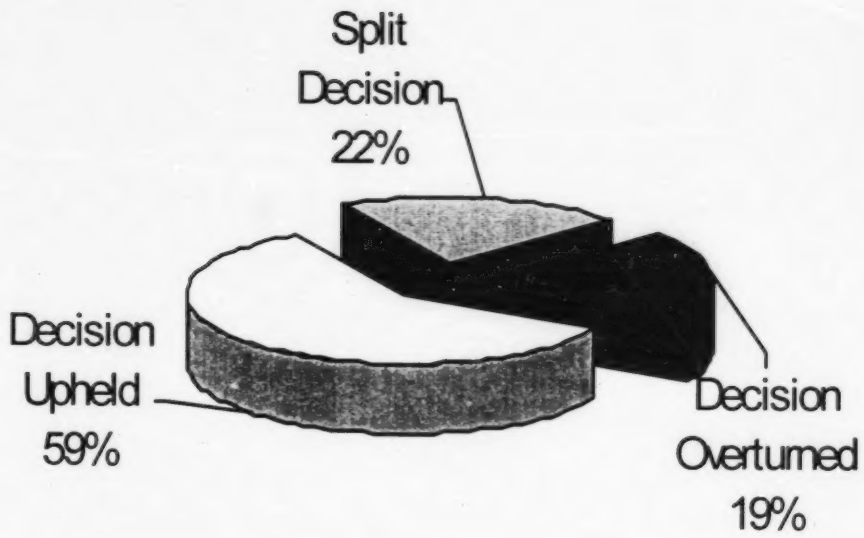
- Confirm, excuse or reduce a fee
- Confirm a decision not to correct personal information or specify how it is to be corrected
- Require a public body to stop collecting, using or disclosing personal information in contravention of the Act
- Require the head of a public body to destroy personal information collected in contravention of the Act

The Commissioner's orders are final and binding, although a party can apply to the Supreme Court of British Columbia for judicial review of the Commissioner's order. Failing this, a public body must comply with the Commissioner's order within 30 days after it is issued.

Between April 1, 2001 and March 31, 2002, the Commissioner released 58 orders. Thirty-four of them upheld the decision of the public body entirely, 11 overturned the public body's decision entirely and success was divided in 13 of them.

Figure 9:

Disposition of Commissioner's Orders
April 1, 2001 and March 31, 2002



Examples of Commissioner's Orders

Coca-Cola sponsorship agreements (Order 01-20 & Order 01-21)

In two decisions, the Commissioner ordered the University of British Columbia and Capilano College to release to their respective student newspapers the remainder of their exclusive sponsorship agreements with Coca-Cola Bottling Ltd. In Capilano College's case, the agreement was between Coca-Cola and an association of post-secondary institutions, including Trinity Western University, Douglas College and Kwantlen University College.

Parts of the agreements had been released to the access applicants but, in the inquiries, Coca-Cola and the post-secondary institutions argued that release of the remainder would be harmful to the financial or economic interests of the institutions and the business interests of Coca-Cola.

The Commissioner ruled that the evidence of harm put forward by Coca-Cola and the colleges and universities was speculative and conclusionary in nature and offered insufficient evidence of harm. He also found that disclosure in the U.S. of similar sponsorship agreements lent weight to the contention that public accessibility does not stop companies from entering into such agreements and noted that Coca-Cola and the post-secondary institutions did not produce any evidence to the contrary.

With respect to the argument that release of the rest of the agreements would harm Coca-Cola's business interests, the Commissioner reminded the parties that information can be withheld for this reason only if it meets the three-part test in s. 21. The Commissioner found that only the first part of the test was met here. He found no evidence to support the argument that release of the agreements would reveal information supplied, as opposed to negotiated, by Coca-Cola and he found there was insufficient evidence of harm as required by the Act.

Grizzly bear kill location data (Order 01-52)

In this case, the Commissioner ordered the Ministry of Water, Land and Air Protection to release the locations of grizzly bear kills to two conservation

groups, B.C.'s Raincoast Conservation Society and the Environmental Investigation Agency, a conservation group based in England.

Grizzly bear kill information is collected by the Ministry from hunters, who are required under the *Wildlife Act* to report the date, location and sex of all grizzly bear kills. The Ministry converts the hunter's description of the location into map co-ordinates, which it uses for management and conservation of the grizzly bear. In response to the access requests, the Ministry had provided kill locations according to Ministry wildlife management units, but refused to release more detailed locations on the grounds release could damage or interfere with the conservation of a vulnerable species within the meaning of s. 18(b) of the Act.

While the Commissioner accepted the Ministry's argument that the grizzly bear is an endangered or vulnerable species, he did not agree that it was reasonable to expect that release of the kill location information could damage or interfere with the conservation of grizzly bears as argued by the Ministry.

The Ministry and the Ministry of Attorney General have applied to the British Columbia Supreme Court for judicial review of this decision.

Actor's contract for advertising services
(Order 01-03)

The applicant had, in 1998, sought access to contracts between the BC Lottery Corporation and well-know actor for the actor's services in television advertisements. The previous Commissioner had upheld the BC Lottery Corporation's decision to refuse access, but the same applicant applied again for access to the same contracts and renewals of those contracts.

The Commissioner decided that, because the matter had been decided before, the applicant was precluded from rearguing his case, having been unsuccessful before the previous Commissioner.

Renewed appeal regarding a settled access appeal
(Order 01-16)

The applicant had, in 1998, sought a review by the OIPC of Simon Fraser University's decision to refuse access to certain information. The applicant agreed

to a settlement of that earlier request, but later made the same access request to the University for the same record.

The Commissioner decided that settlement during mediation is not a decision to which legal doctrines precluding a re-opening of the matter can apply. He also held, however, that the Commissioner has the authority under Part 5 of the Act, to control abuse of the review and inquiry process by applicants. Fairness is the touchstone in determining whether a repetitive access request should be allowed to proceed through the review and inquiry process. The Commissioner decided the applicant's second request was an abuse of the process and that fairness did not require that the applicant be permitted to insist that the process be followed once again.

First Nations and fee waivers
(Order 01-24)

The applicant, who was a researcher for a First Nation, sought a public interest fee waiver from the Ministry of Transportation for access request involving a possible claim against the provincial government. The Commissioner held that just because the applicant is or represents a First Nation, it is not necessarily in the public interest to waive a fee under s. 75(5)(b) of the Act. It is necessary for the records themselves to relate to a matter of public interest. The Commissioner upheld the Ministry's decision to refuse a fee waiver.

Water quality issues are of public interest
(Order 01-35)

The applicant community group had requested records relating to a forest company's proposals for logging road construction and timber cutting in a specific watershed. The community group was concerned about the effect of logging activities on the quality of water that supplied the community. The Commissioner decided that, even though only a small number of families in one watershed was affected, the records relate to a matter of public interest, *i.e.*, the environment in the local watershed. The Commissioner also decided, however, that the Ministry was within its rights to refuse a fee waiver, in light of the fact that the applicant had made numerous previous access requests and the Ministry had not charged a fee.

7.0 Providing Advice

Under section 42 of the Act, the Commissioner has the mandate to comment on the access or privacy implications of proposed legislative schemes or programs, automated systems for the collection, management or transfer of personal information, record linkages or any other matter that impacts on privacy or open government.

Since its inception, the approach of the OIPC is to work collaboratively with public bodies to support them in the discharge of their legislative obligations. Much of the advice-giving role is fulfilled through normal course of business dialogue between a public body and a Portfolio Officer.

In an ideal world, public bodies would directly consult the Commissioner before any legislation, program or technology impacting access and privacy rights was implemented. And, in most cases, this is what occurs. Comments are normally provided to the public body seeking advice, but occasionally they are posted on the OIPC website, if the issue is of significant public interest.

In developing new or changing existing programs and policies, public bodies are encouraged to conduct a Privacy Impact Assessment before the program or change is implemented. A Privacy Impact Assessment is a tool by which public bodies assess compliance with the privacy protections set out in Part 3 of the Act. Privacy Impact Assessments are generally conducted before any new database; legislation, policy, program or technology is implemented that involves the collection, use and disclosure of personal information. It is normal practice for the OIPC to review and comment on Privacy Impact Assessments submitted by public bodies.

Issues needing scrutiny often come to the attention of the OIPC outside of the direct consultation process, for example through the media, through a complaint or through the grapevine. In such cases, the OIPC will contact the public body to obtain relevant information and make recommendations to address any access or privacy issues identified.

Finally, the OIPC publishes guidelines for public bodies to consider when making decisions that have potential access or privacy concerns. Those include guidelines concerning data service contracts, public video surveillance, research agreements and automating information systems.

The following snapshot illustrates the range of issues commented on by the OIPC:

- Anonymizing public reports issued by the Office of the Police Complaints Commissioner
- The BC Ferries reservation system
- Access to core common data on all health providers by HealthNet BC
- The BCMA policy on Physicians and Office Visits
- Disclosure of personal information pursuant to collective agreements
- Access to hospital files by hospital chaplains
- The National Diabetes Surveillance System
- The MOU between the Ministry of Social Development and Economic Security and Citizenship and Immigration Canada
- The security review of the PharmaNet System
- Proposed federal regulations under the *Personal Information Protection and Electronic documents Act*
- The Anti-Terrorism Act
- MOU between ICBC and Canadian Blood Services
- The proposal by the Vancouver Police Department to place public surveillance cameras in the downtown eastside
- The Canadian Institute for Health Information's privacy policies and practices
- Hospital representation agreements
- The Ministry of Children and Family Development's Practice Guidelines for Assessing Parental Substance Use as a Risk Factor in Child Protection Cases
- Intelligent transportation systems
- Video surveillance on public buses
- Proposed prostitute DNA databank

Training and Development

Section 42 of the Act gives the OIPC general responsibility for monitoring how the Act is administered to ensure its purposes is achieved. As part of this responsibility, the OIPC provides training to public bodies in the form of workshops, seminars and speeches. Typical training sessions cover "the basics" of access and privacy, including response timelines, duty to assist, exceptions to disclosure, contents of response, collection, use and disclosure of personal information, security and retention.

Examples of OIPC training initiatives include:

- A one-day workshop for information and privacy managers of policing agencies, Victoria
- Presentation to the Vancouver Hospital Staff, Vancouver
- Participation at the Continuing Legal Education Conference, Vancouver
- Seminar with the Provincial Brain Injury Program, Victoria
- Privacy impact assessment training sessions, Victoria
- Seminar with the Columbia Basin Trust on privacy issues pertaining to data linkages, Nelson
- Seminar to the BC Cancer Agency, Victoria
- Workshop to university and college information and privacy managers, Victoria
- Co-presenters with the Criminal Justice Branch to a regional meeting of administrative crown counsel, Prince George
- Training seminar with the College of Teachers regarding disclosure of discipline information, Vancouver
- Access and privacy training session with Ministry of Forests, Victoria

8.0 Informing the Public

One of the responsibilities the OIPC takes very seriously is its mandate to educate the public about their access and privacy rights. This function is fulfilled through speaking engagements, participation in conferences, seminars and workshops, through the production of collateral education material such as brochures and through the OIPC website.

The Commissioner was a keynote speaker and primary participant at several major access and privacy conferences. Among those were presentations to the:

- Freedom of Information and Protection of Privacy Association Annual Conference
- Health Records Association of BC Conference
- Continuing Legal Education conference on Suing and Defending Government
- Canadian Institute Conference on Managing Privacy of Health Information
- Canadian Institute Conference on Security and Privacy for Online Government in Toronto.

In addition, staff from the OIPC participated in a number of public outreach activities, delivering speeches, workshops and seminars to a number of groups, among them:

- University of British Columbia education students
- University of Victoria public relations students
- Simon Fraser University political science students
- Canadian Alarm and Security Association
- BC Magazines Publisher's Association
- Centre for Collaborative Government
- Canadian Association for Practical Study of Law in Education
  BC Council of Administrative Tribunals
- Interns of the Legislative Assembly of BC

9.0 Financial Statement

Operations - For the year ending March 31, 2002

	Budget	Actual
Total Salaries and Benefits	$1,666,000	$1,641,139
Total Operating Costs	$ 693,000	$ 587,152
Total Recoveries	($15,000)	
Total Voted Appropriation	**$2,344,000**	**$2,228,291**
Unused Appropriation		**$ 115,709**

Capital Assets -For the year ending March 31, 2002

	Budget	Actual
Opening Cost of Tangible Capital Assets		$ 221,142
Appropriations for purchase of capital assets	$ 15,000	$ 14,870
Capital asset amortization	$ 18,000	($ 14,791)
Accumulated Amortization		($ 194,547)
Closing Cost of Tangible Capital Assets		$ 26,674

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Mailing Address:

PO BOX 9038, Stn Prov. Gov.
Victoria, BC
V8W 9A4

Location:

4th Floor, 1675 Douglas Street
Victoria, BC

Telephone: (250) 387-5629

Fax: (250) 387-1696